Die Notfalldiskette von Windows NT

Die Notfalldiskette von Windows NT

Carsten Doil

Immer wieder erleben wir in Support-Fällen zu Microsoft Windows NT, daß die betroffenen Benutzer nur ungenügenden Gebrauch von der Sicherungsmöglichkeit der zentralen Konfigurationsdatenbank Registry machen. Daher sollen an dieser Stelle technische Hintergründe, Pflege und Einsatzmöglichkeiten näher erläutert werden.

Jeder Benutzer wird bei der Installation von Windows NT zur Erstellung einer Notfalldiskette aufgefordert. Leider wird diese Option sehr häufig ignoriert oder diese erste Version später, im laufenden Betrieb des Rechners, nicht aktualisiert. Dabei ist diese Diskette und die Kopie auf der Festplatte im Systemverzeichnis das wichtigste Hilfsmittel um ein zer- oder gestörtes System wiederherzustellen oder zu einem bestimmten Systemstand zurückzukehren.

Besonders wichtig für die Systemintegrität sind dabei die beiden Teile SYSTEM (Hardware- und Treiber-Konfiguration) und SOFTWARE (Konfiguration der installierten Software). Diese sind etwa mit den Dateien `system.ini` und `win.ini` in MS Windows 3.x vergleichbar. Wenn ein Bereich in diesem Registry-Teil nicht stimmt, kann es zu Fehlern in der Ausführung von Programmen bis zum Systemabsturz kommen. Deshalb sollte man die Registry regelmäßig sichern, um sich zeitaufwendige Neu-Installationen und -Konfigurationen zu ersparen.

Technischer Überblick

Im Verzeichnis `%SystemRoot%\System32\Config` (wobei mit `%SystemRoot%` das Installationsverzeichnis, meist `c:\winnt`, bezeichnet wird) werden die Bestandteile der Systemkonfiguration (Registry) gespeichert. Mit Außnahme der Datei `Ntuser.dat` die sich im Verzeichnis `%SystemRoot%\Profiles\%USERNAME%` (`%USERNAME%` ist der Benutzername des aktuell angemeldeten Benutzers) befindet:

Registrierungsstruktur	**Dateiname**
HKEY_LOCAL_MACHINE\SAM	Sam (Sam.log, Sam.sav)
HKEY_LOCAL_MACHINE\Security	Security (Security.log, Security.sav)
HKEY_LOCAL_MACHINE\Software	Software (Software.log, Software.sav)
HKEY_LOCAL_MACHINE\System	System (System.alt,System.log,System.sav)
HKEY_CURRENT_CONFIG	System (System.alt,System.log,System.sav)

HKEY_USERS\.DEFAULT	Default (Default.log, Default.sav)
(nicht assoziiert)	Userdiff (Userdiff.log)
HKEY_CURRENT_USER	Ntuser.dat (Ntuser.dat.log)

Tab. 1: Zuordnung von Registry-Struktur und Dateien

Dabei stellen die Dateien ohne Erweiterung den aktuellen Stand dar, `.log`-Dateien werden als Transaktions-Logs bei Änderungen verwendet, `.sav`-Dateien sind Sicherungskopien nach Abschluß des textbasierten Setup-Vorgangs, `system.alt` wird ebenfalls (wie `system.log`) als Absicherung bei Änderungen am SYSTEM-Teil benutzt und `userdiff` wird für die Umstellung von NT 3.x-Benutzerprofilen gebraucht.

Die gesamte NT-Systemkonfiguration setzt sich also aus fünf Teilen zusammen, die in einem speziellen, mit einem Text-Editor nicht bearbeitbaren, Format gespeichert sind. Normalerweise ist dies auch nicht nötig, da alle Veränderungen über die Konfigurations- (Systemsteuerung, Programme in `Start->Programme->Verwaltung`) und Installations-Programme vorgenommen werden. Für die die direkte Bearbeitung stehen standardmäßig die beiden Werkzeuge `regedit.exe` und `regedt32.exe` zur Verfügung. Details zur Nutzung, Änderung und Verwendung kan man in [1] nachlesen.

Das Programm `RDISK.EXE`

Das Standardwerkzeug für die Sicherung der Registry-Dateien ist das Programm `rdisk.exe`. Mit diesem Programm kann man die gesamte oder auch nur einen Teil der Registry auf die Festplatte und/oder auf eine Diskette sichern. Das Zielverzeichnis `%SystemRoot%\repair` auf der Festplatte ist dabei fest vorgegeben.

Gesichert werden die folgenden Dateien (siehe [2]):

Dateiname	**Inhalt**
Autoexec.nt	Kopie von `%systemroot%\System32\Autoexec.nt` zur Initialisierung der MS-DOS-Umgebung
Config.nt	Kopie `%systemroot%\System32\Config.nt` zur Initialisierung der MS-DOS-Umgebung
Default._	Registrierungsschlüssel `HKEY_USERS\DEFAULT` , komprimiert
Ntuser.da_	Komprimierte Version von `%systemroot%\Profiles\DefaultUser\Ntuser.dat` . Muß diese Datei wiederherstellt werden, wird hierzu die Datei `Ntuser.da_` verwendet
Sam._	Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SAM` , komprimiert
Security._	Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SECURITY` , komprimiert
Setup.log	Protokoll der installierten Dateien sowie CRC-Prüfungsinformationen zur Verwendung während des Wiederherstellungsvorgangs. Bei dieser Datei handelt es sich um eine schreibgeschützte, versteckte Systemdatei, die nur sichtbar ist, wenn Sie im Arbeitsplatz oder im Windows NT-Explorer die Anzeige aller Dateien eingestellt haben
Software._	Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SOFTWARE` , komprimiert
System._	Registrierungsschlüssel `HKEY_LOCAL_MACHINE\SYSTEM` , komprimiert

Tab. 2: Die Dateien im Repair-Verzeichnis und auf der Reparatur-Diskette

Die Speicherung der Daten geschieht in komprimierter Form und kann bei Bedarf mit den

Die Speicherung der Daten geschieht in komprimierter Form und kann bei Bedarf mit den Kommandozeilen-Programm `expand.exe` auch manuell entpackt werden.

Das Programm hat zwei Ausführungsoptionen:

1. **rdisk /s**: Damit werden alle oben genannten Dateien in das Repair-Verzeichnis gesichert. Anschließend kann auf Wunsch die Reparatur-Diskette erstellt werden. Diese vollständige Sicherung kann, z.B. bei großen Servern, nicht auf eine Diskette passen, da die SAM sehr groß werden kann. In diesem Fall muß man die Dateien manuell auf mehrere Disketten kopieren
2. **rdisk**: Damit startet man das Programm im interaktiven Modus.
   a. Aktualisieren: Speichert alle oben genannten Dateien. Mit **Ausnahme** von SAM und SECURITY
   b. Erstellen: Erstellt eine Reparatur-Diskette. Kopiert also den Inhalt von `%SystemRoot%\repair` auf eine Diskette
   c. `Beenden` und `Hilfe` sind selbsterklärend

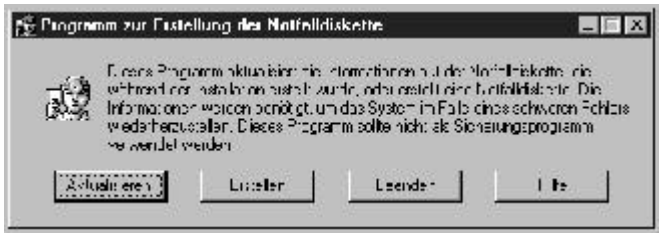

Abb. 1: Der interaktive Modus von `rdisk.exe`

Manchmal kann es sinnvoll sein mehrere Versionen (History) von Sicherungen anzulegen und aufzubewahren. Dazu verwendet man einfach mehrere Disketten und kopiert vor Ausführung von `rdisk.exe` die Dateien aus `%SystemRoot%\repair` in ein anderes Verzeichnis (z.B. `%SystemRoot%\repair.<Erstellungsdatum>`). Dabei sollte immer darauf geachtet werden, daß auf die Sicherungen, wie auch auf die Diskette(n) nur authorisierte Personen Zugriff haben.

Die gesicherten Daten im Notfall benutzen

Grundsätzlich sollte man die oben beschriebene Sicherung regelmäßig, z.B. wöchentlich, durchführen. Außerdem ist es ratsam vor größeren Systemveränderungen wie Ein- oder Ausbau von Hardware, (De-)Installation von Software, Treiber-Updates u.ä. eine Sicherung anzulegen. Wenn dann der Fall eintritt, daß das System nicht mehr sauber läuft oder beim Boot-Vorgang sogar abstürzt, dann muß die Sicherung durch den Reparatur-Modus zurückkopiert werden.

Der Reparaturvorgang

Um Windows NT im Reparatur-Modus zu starten, benötigt man die Installations-CD und die drei Installations-Disketten. Diese kann man mit dem Installationsprogamm `winnt.exe /ox` (DOS-Version) bzw. `winnt32.exe /ox` (Win95/NT-Version) jederzeit erstellen. Um nun in den Reparatur-Modus zu gelangen muß man von den Installations-Disketten gebootet und dabei folgende Dialoge durchlaufen werden:

- Boot-Vorgang mit den Disketten 1 und 2 bis zum ersten Dialog
- Auswahl des Reparatur-Modus mit Taste **R = Reparieren**
- Wahl der Reparatur-Option (mit Pfeil-Tasten auf und ab, Eingabe-Taste für Auswahl benutzen). Es gibt noch drei weitere Optionen außer der Registry-Reparatur, deren Bedeutung hier nicht näher erläutert werden soll (siehe Onlien-Hilfe mit F1):

```
[X] Untersuchen der Registrierungsdateien
[ ] Untersuchen der Startumgebung
[ ] Überprüfen der Windows NT-Systemdateien
[ ] Überprüfen des Bootsektors
Fortsetzen (gewählte Aktion(en) durchführen)
```

- Dann, wie von der Installation gewohnt, die dritte Installationsdiskette verarbeiten (Auswahl und Start der Festplattenadapter-Treiber usw.)
- Angabe, ob eine Notfalldiskette vorliegt und diese benutzt werden soll. Alternativ kann nach einer vorhanden NT-Installation auf der Festplatte gesucht und die dort im Repair-Verzeichnis gefundenen Dateien verwendet werden.
- Das System wird nun nach Defekten untersucht und danach können die Teile der Registry zur Wiederherstellung gewählt werden (mit Pfeil-Tasten auf und ab, Eingabe-Taste für Auswahl benutzen, F1-Taste für Online-Hilfe), z.B.:

```
[X] SYSTEM (Systemkonfiguration)
[ ] SOFTWARE (Software-Informationen)
[ ] DEFAULT (Standard-Benutzerprofil)
[ ] NTUSER.DAT (Profil für neuen Benutzer)
[ ] SECURITY (Sicherheitsrichtlinien) und
SAM (Benutzerkontendatenbank)
Fortsetzen (gewählte Aktion(en) durchführen)
```

- Vorgang durch Neustart des PCs abschließen.

Damit ist der Reparatur-Vorgang abgeschlossen und die alten Teile der Registry stehen wieder zur Verfügung.

Nutzung eines Zweit-System

Eine weitere wichtige Möglichkeit für die Wiederherstellung eines nicht mehr funktionirenden Systems ist das Booten von einem zweiten sogenannten Notfall-System. Dieses kann sich auf einer Extra-Partition der Festplatte oder auch auf einem ZIP-Lauf-werk befinden. Damit erhält man kompletten Zugriff auf die Platte mit dem kaputten NT-System und kann, außer der Registry, auch andere Dateien ersetzen, das Dateisystem prüfen, ein Backup von Band zurückspielen o.ä., ohne vom laufenden Betriebssystem behindert zu werden. Gerade bei Server-Systemen bietet sich dies an. Als sehr flexibel hat sich dabei die Variante mit einem externen ZIP-Laufwerk (SCSI-Version) herausgestellt, da diese an jeden PC mit SCSI-Schnittstelle angeschlossen und von einer Diskette gestartet werden kann. Eine Kopie einer solchen ZIP- und Bootdiskette ist auf Anfrage an die E-Mail-Adresse pc-hilfe@rus.uni-stuttgart.de erhältlich.

Weitere Werkzeuge

Auf der Microsoft NT Resource Kit Begleit-CD sind diverse weitere Programme für die Bearbeitung der Registry enthalten (siehe [1]). Diese CD befindet sich auch im Lieferumfang von MS-TechNet (siehe Artikel in dieser BI.). Allerdings sollte man bei der Nutzung dieser Werkzeuge sehr vorsichtig sein, um sich sein System nicht durch Tests zu zerstören. Machen Sie daher vorher auf jeden Fall eine Sicherung. Sehr interessant ist die Datei `Regentry.hlp` , in der die Bedeutung der Registry-Einträge einzeln erläutert werden.

Literatur

MS Windows NT Workstation 4.0 Resource Kit, MS Press Verlag, ISBN 3-86063-241-8 (oder auch in MS-TechNet):

[1] Kapitel 23-26
[2] Kapitel 20

Carsten Doil, NA-4512
E-Mail: doil@rus.uni-stuttgart.de